Naval War College Review

Volume 56
Number 2 *Spring*

Article 8

2003

Small Navies and Network-centric Warfare—Is There a Role?

Paul T. Mitchell

SMALL NAVIES AND NETWORK-CENTRIC WARFARE

Is There a Role?

Paul T. Mitchell

Is there a place for small navies in network-centric warfare? Will they be able to make any sort of contribution in multinational naval operations of the future? Or will they be relegated to the sidelines, undertaking the most menial of tasks, encouraged to stay out of the way—or stay at home? If the recent experience of the Canadian navy is any guide, small navies have every right to be concerned about their future in network-centric operations. For while the Canadian navy has achieved a high degree of success within U.S. naval formations, it has done so only by virtue of highly privileged access. To date, the challenges posed by the revolution in military affairs in general and network-centric warfare (NCW) in specific have been framed in terms of technology and investment.[1] The allies and partners of the United States are lagging in technology and investment therein, and they need to make significant capital investments in order to catch up. Worse, "dynamic coalitions," developed rapidly to deal with crisis situations, may become the most common form of military cooperation. In such coalitions, detailed, prearranged plans and doctrine are likely to be entirely absent. Partners will have had little in-depth operational experience or knowledge of their own capabilities. Technical standardization will be low; national logistical support may be limited or entirely absent. Significantly, there may be serious questions regarding the professionalism of personnel participating in these coalitions.[2]

Dr. Mitchell has been director of academics at Canadian Forces College in Toronto since 2001, as well as an adjunct fellow at the Centre for Military and Strategic Studies, University of Calgary. After receiving a B.A. (Honours) at Wilfred Laurier University and an M.A. in war studies at King's College, University of London, he earned in 1995 a Ph.D. in political studies from Queen's University in Kingston, Ontario. Before joining the Canadian Forces College he lectured at Queen's and the Royal Military College and served at the Centre for Foreign Policy Studies at Dalhousie University (Halifax, Nova Scotia) and the Pearson Peacekeeping Centre (Cornwallis, Nova Scotia). He is a coeditor of Multinational Naval Cooperation and Foreign Policy in the 21st Century *(1998) and author of numerous journal articles and essays in collected works.*

Naval War College Review, Spring 2003, Vol. LVI, No. 2

How dynamic coalitions will function in network-centric warfare is undoubtedly problematic. One commentator has recently suggested that the nature of NCW may ultimately result in more unilateral (or virtually unilateral) U.S. operations, such as that recently conducted in Afghanistan. In effect, the risk of "clueless coalitions" may drive the United States, however unwillingly, toward a more unilateralist military policy, irrespective of that enunciated in its national security strategy.[3] The Joint Chiefs of Staff have called for a more "tailored approach to interoperability that accommodates a wide range of needs and capabilities" without implying "access without restraint."[4] In the unstructured environment implied by the concept of dynamic coalitions, however, the policy restraints upon information sharing, surely the heart of network-centric warfare, may be considerable. As Thomas Barnett has pointed out, "Not only will our allies have little to contribute to the come-as-you-are party, they won't be able to track the course of the conversation."[5]

This article examines the nature of NCW, the challenges it presents to coalition operations, and some recent developments that seek to overcome these challenges. It uses the Canadian navy's recent and ongoing experience of directly integrating into U.S. carrier battle group operations as a test case. The article finds that the principal challenges that will be raised by NCW are not likely to be technical ones, although undoubtedly these will be formidable. Rather, the most challenging issues for all navies, and small ones in particular, stem from policy. If Canada's example is typical, navies that have less well developed relationships with the U.S. Navy are likely to confront such crippling difficulties in integrating into NCW-dominated operations as to be excluded from them.

THE NATURE OF NCW

Much of what has been revolutionary in the revolution in military affairs is not so revolutionary from a naval perspective.[6] Navies have been working with information technology since 1957, when the CANUKUS Naval Data Transmission Working Group, after three years of deliberations, ratified the technical standard for data exchange.[7]

Link 11 is more or less standard among Western navies. Primarily used to share tactical information so as to develop what is now known as a "common operational picture" within a task group, Link 11 data is also used by the U.S. Navy to transmit certain engagement orders. However, for many reasons, Link 11 is relatively slow. Because of significant lag times between target detection and the posting of data onto the Link network, its information is not of fire-control quality. Further, it passes to linked ships only the data that has already been processed on board the contributing ship. This occasionally leads to duplicate tracks or conflicting information about the same target. Link 11 demands a high

degree of professional competence on the part of track coordinators in order to keep the operating picture "clean."[8]

Network-centric warfare aims at increasing the efficiency of the transfer of maritime information among participating units (or nodes). By optimizing the efficiency of operations through information exchange, even small naval formations can generate additional combat power.[9] Data is manipulated by a series of dynamic and interlinked "grids": sensor grids gather the data, information grids fuse and process it, and engagement grids manage the operations generated.[10] Improved operational efficiency results not only from the increased speed at which operations can proceed but also from the "self-synchronization" that is generated between units.[11] This speed and synchronization ultimately merge the strategic "recognized maritime picture" with common operational and tactical pictures.[12] For example, in Canadian ships, the recognized maritime picture is provided to ships by shore-based facilities, whereas ship-based sensors and tactical data links generate local information. At the moment, neither informs the other, which can often lead to discrepancies. With the merging of information into a common pool distributed by linked systems, plans and operations will become much more dynamic. They will be able to react instantly to changes in the battle space, by virtue of their enhanced awareness of them. For navies having this capability, the result is a competitive advantage, an ability to "lock in success" while locking out enemy initiative.[13]

The original requirement to increase reaction speeds arose in the Cold War in order to deal with hypothesized regiment-sized air attacks on surface ships; the present impetus for speed and synchronization is the return of fleet operations to their traditional setting, in and around the littorals. The sheer density of maritime and air traffic, the presence of naval, commercial, and recreational maritime vehicles, results in a level of complexity that blue-water operations rarely encounter. This web of activity is made all the worse by the influence of microclimates, complex oceanography, and unique geographical features. Finally, in the littoral, there are few places where a warship does not stand out, whereas defenders are afforded a multitude of opportunities to hide their forces, whether geographically or through deception, basing them on nonnaval platforms.[14] In effect, naval forces are forced onto an "asymmetrical" battlefield in the littorals.[15]

In response, networked operations permit enhanced speed and synchronization, which generate predictive planning and preemption, resulting in proactive, "maneuverist," effects-based operations; integrated force management, allowing synchronization of missions and resources; and execution of time-critical missions, employing "near optimal weapons pairings."[16]

The most explicit technological development stemming from these conceptual underpinnings has been "cooperative engagement," which passed its operational evaluation trials in September 2001.[17] Cooperative engagement, like Link 11, seeks to develop the common operational picture; unlike Link 11, however, it also aims to coordinate threat decisions in real time. Further, it also attempts to distribute fire-control-quality information to participating network nodes.[18] Cooperative engagement improves a force's ability to share data, even that of a fragmentary nature. For example, because of stealth technology or terrain-masking effects, a ship's sensors may be unable to collect precise and complete information on a particular target. In a formation equipped with cooperative engagement, ships would automatically cue other sensors within the formation, producing a more detailed picture. All this information could then be pooled with the data collected by other more distant ships to assemble a "composite picture" of the target that no single ship would have been able to generate. Units might thereby receive fire-control-quality information on targets outside their sensor horizons; they could fire weapons before threats appeared to them, allowing engagements to take place at maximum distance from the targets.[19] The end result of all this would be a considerable increase in the time available to make decisions—more time to assess threats and respond—and operations faster than the opponent can sense and respond to himself. Cooperative engagement is not the only technical development speeding up the pace and efficiency of naval operations within the U.S. Navy. Much like the private business world in the last five years, the U.S. military has taken advantage of the Internet to improve the flow of information. The Defense Message System, backed up by the Secret Internet Protocol Routing Network (SIPRNET), has introduced a series of World Wide Web–based applications such as e-mail with attachments, "chat rooms," and web pages.[20] SIPRNET in particular seems to have had a revolutionary impact on the planning and conduct of operations within the U.S. military. It has transformed laborious manual procedures into rapid electronic ones. This became most evident during Operation ALLIED FORCE, when the sheer amount of paperwork forced planners to use electronic formats, "which were substantially easier to create, pass via e-mail, and maintain visibility on." As superiors appended their comments on forwarded messages, it became simpler to track the evolution of commanders' intentions as well.[21] Even "chat rooms," so ubiquitous among idle teenagers, have a distinctly revolutionary aspect in that they permit the transmission of information (along with attachments of imagery and

The underlying trouble is that the guiding principle of NCW is to increase speed and efficiency, whereas coalitions are always about scarcity.

other intelligence) without radio communication, thus preserving communications security within a theater.[22]

Video teleconferencing (VTC) has also led to "compressed command and control processes" through its ability to span the strategic, operational, and tactical levels. It is particularly useful for staffs that are widely dispersed geographically.[23] A previous Sixth Fleet commander, Vice Admiral Dan Murphy, called VTC "the wave of the future." Video teleconferencing obviates the need to collocate staffs and reduces ambiguity in commanders' intentions.[24] VTC and chat functions collectively permit "distributed collaborative planning," which seeks to assemble problem solvers for rapid and effective response to time-critical situations, while providing access to and ensuring the availability of information resources.[25] Aircraft carrier battle groups are inherently dynamic

FIGURE 1

Time	Event
05:00	Receive unit operational reports
08:00	Brief battle group commander
09:00	Brief JTF commander
10:00	Warfare commanders' coordination board
13:00	Planning cell meetings
18:00	Release commander's intentions and situation report messages
20:00	Units receive commander's intentions
00:00	Units release operational reports

given the constant flow through them of ships, personnel, and new technology. It is necessary to control this dynamism rather than be overwhelmed by it; accordingly, a battlegroup deployment involves a meticulous process of training and planning through which all participating units and individuals become familiar with the synergies between processes, procedures, and systems. The product is a specified "battle rhythm" (see figure 1). This battle rhythm requires that everything within the group, system, individual, or ship, "not have an adverse effect on communications or information flow." To this end, the battle group proceeds through a series of subunit and unit training exercises. These culminate in the "comprehensive task unit exercise" that certifies the battle group for basic functions and a final "joint task force exercise" that combines the CVBG with other formations, such as amphibious groups and allied formations.[26]

ALLIED FORCE and subsequent operations in Kosovo are widely hailed as beginning the introduction of network-centric operations, and ENDURING FREEDOM in Afghanistan has laid to rest many of the criticisms. This is especially so since that operation saw the confrontation of a high-tech military against a ragtag, guerrilla-type army:

> The Afghanistan operation may ultimately prove to be a boon to the Department of Defense's revolution in military affairs, in which the prize is not territory but information. Only after a clear picture of the battlefield is assured—and that shared with as many weapons platforms as possible—can the maximum potential of PGMs and other high tech weaponry be unleashed both militarily and politically.

Particularly impressive has been the manner in which information from a wide variety of sources has been processed and fused for both air and ground forces, thus permitting midcourse updates, engagement zones, "moving target options," and cockpit target imagery.[27]

Equally evident, however, was the initial lack of allied participation in the most secret and demanding operations. While this might have stemmed from a general lack of allied logistical lift, other possibilities must also be considered. As Vice Admiral Arthur K. Cebrowski, the "godfather" of network-centric warfare, has noted, while the United States wants its partners to be as interoperable as possible, "not being interoperable means that you are not on the net; so you are not in a position to derive power from the information age."[28]

NCW AND INFORMATION BARRIERS

Getting on the net may not be a simple process at all for allies and coalition partners. Essentially, these nations face two distinct challenges: network access may be hampered by technical incompatibilities inherent in their force structures, but it may be obstructed also by design.[29]

Recent operations in the Balkans have underscored the difficulties of meeting American expectations for rapid, information-dense operations. During operation SHARP GUARD, conducted by NATO and the Western European Union in the mid-1990s, the ability of a ship to compile an operational picture was limited at times to its own horizon. Further, the commander of NATO Naval Forces South, in Naples, initially had no timely access to information being collected by units under his command.[30] During ALLIED FORCE, "existing data networks were not adequate to support the flow of information of . . . data among key nodes of the NATO information grid." Further, the United States was unable to pass along "high-fidelity data"; the alliance experienced accordingly difficulties attacking time-sensitive targets, "because of the need for rapid exchange of precision targeting data and continuous precision updates from sensor to shooter until the target is destroyed."[31]

Although some of these issues later found technical solutions (SHARP GUARD units and command centers eventually received old U.S. Navy Joint Operational Tactical System terminals, for example), the "need for speed" in network-centric operations places the whole notion of multinational operations at risk. Interoperability barriers may exclude even close allies. Connectivity problems

are the "equivalent of changing to a different railway gauge at each national border";[32] high-tempo operations therefore ultimately become hostages to the units with the slowest information and decision cycles.[33] Just as pressing and in the long term even more damaging than technology differentials may be lack of physical access. Liaison officers have traditionally been exchanged by militaries to ensure the transmission of information among partners, particularly when there are interoperability problems.[34] Today, liaison officers are often unable to enter U.S. command centers because of security restrictions.[35] Technology itself may ultimately lead to the electronic equivalents of these physical barriers.

The growing use of video teleconferencing directly raises this issue, because of the classified information frequently involved. In order to access a VTC link, "all users must be on the same level of classification of network and have access to the information on the network."[36] The lack of timely written documentation and the instantaneous, experiential nature of VTC hinder any participation by those not on the network.[37] As Major General John Kiszely of the British army has pointed out more broadly, "Full interoperability between forces would depend upon integrated collaborative planning based on the maintenance of a common operating picture and common intelligence inputs. Without appropriate digital communications, this would not be practical, and made all the more unlikely because the U.S. SIPRNET is NOFORN [not releasable to foreign nationals]."[38] Thus, network-centric operations in a coalition or alliance environment may ultimately hinge on information releasability rules and the ability to exchange information between networks of different security classifications.

Much of what has been revolutionary in the revolution in military affairs is not so revolutionary from a naval perspective.

The underlying trouble is that the guiding principle of NCW is to increase the speed and efficiency of operations, whereas coalitions are rarely concerned about combat efficiency. Coalitions are always about *scarcity*—in terms of operational resources, political legitimacy, or both. The trade-off is always in terms of political influence over operational considerations; in coalitions, politics frequently trump efficiency. Neither is information releasability policy oriented around efficiency, but rather security. "Information release and control must be conducted in a manner that prevents damaging foreign disclosure[;] this capability must be demonstrated to information owners" before any transfer can be effected.[39] Information, and what it may imply about the systems that collected it, may be too sensitive to be entrusted to others.

In the absence of clearinghouses for information, information disclosure between nations is typically a tedious and cumbersome procedure.[40] Further, because the long-term effect of individual disclosures can be difficult to ascertain

and because the career impact of improper disclosure is so serious, "commanders often choose stringent release rules to avoid problems."[41] In this way, releasability concerns have dictated separated networks operating at different tempos. As Brigadier General Gary Salisbury, director of command, control, and communications systems for U.S. European Command, characterized the situation in September 2001,

> How do [combined planners] get these national communication and information needs and fit these into a coalition environment? The bottom line is we are generally operating two different networks at two different security levels. We run our networks at a coalition releaseability level that's basically unclassified.[42]

It is ultimately these information security policies that prevent allies and partners from operating at the same speed as the American military. Many of the problems of interoperability between allies and coalition partners are the same as those encountered in joint interoperability. Some have suggested that lessons learned from the latter can be applied to coalitions.[43] Nevertheless, the intervening variable, not present in joint situations, is that of international politics. The transnational element—particularly as it affects information security—makes coalition and alliance interoperability an order more difficult than joint interoperability.

It would be a gross overstatement to claim that the United States is unconcerned by the issue of information releasability. Throughout the 1990s and still today, the United States has sponsored Joint Warrior Interoperability Demonstrations (JWIDs), intended to seek technical solutions to common and pressing interoperability problems. These demonstrations have identified several technical solutions; for instance, "Radiant Mercury" and "SIREN" (Secure Information Release Environment) decision-support software, which speed up the sanitization and declassification of secret documents.[44] The 1996 JWID identified the "Coalition Wide Area Network" (CWAN) as a "golden nugget." CWAN permits establishment of a common operational picture at a "coalition secret" level. Separated (though not entirely) from the SIPRNET by software firewalls and gateways, CWAN was initially introduced in the multinational RIMPAC ("rim of the Pacific") exercise series and is currently being widely used elsewhere as well.[45] Finally, the U.S. assistant secretary of defense for command and control has sponsored a series of workshops and seminars among a working group composed of Australia, Canada, Germany, Britain, and the United States, with France as an observer. The working group seeks to identify the core needs of information exchange and to establish common doctrine and procedures prior to any operation.[46]

Dwight D. Eisenhower famously remarked, "Allied Commands depend on mutual confidence."[47] Like relinquishing command and control, releasing sensitive information is an act of trust between states surpassed only, perhaps, by placing troops under even the limited control of an ally; releasing closely held knowledge places technology, operations, and even personnel at risk.[48] "Trust involves a willingness to be vulnerable and to assume risk. Trust involves some form of dependency."[49]

Thus, we can expect that just as nations have always been unwilling to place complete control of their troops under the control of foreign nations, they will be unwilling to share completely all information they have: "As close as . . . Canadian and British allies are in common interests and objectives, there will always be limits to sharing the most highly classified information with these nations."[50] In the past, this reluctance did not typically jeopardize operations. However, in network-centric warfare information is the cornerstone of all action; the existence of separate networks operating at different speeds will have an undeniable impact on battle rhythms.

The United States is certainly willing to share most of its information with certain partners. For forces of nations not in this privileged club, integration into American networks will be increasingly difficult, depending on how often they operate with the U.S. forces and the degree of trust extended to them. Forces not permitted to take part in planning will ultimately be restricted simply to taking orders—possibly to assume high-casualty or politically distasteful roles.[51] The added risk is that multinational operations will become more and more circumscribed, that allied participation will be accepted only under the most restrictive circumstances. The United States is unlikely to hamstring its own military forces or to slow its implementation of network-centric warfare given its obvious benefits. It may decide simply to "pass" entirely on alliance participation.[52] Information releasability policy would ultimately decide, then, not only the shape and nature of naval coalitions but possibly even their very existence.

CANADIAN SHIPS IN AMERICAN CVBGS

One can get a sense of the challenges facing coalition naval network-centric warfare by examining the integration of Canadian warships into U.S. aircraft carrier battle groups. In some respects, this case represents the crucible, for any difficulties faced by Canadians are likely to be considerably more intense for navies outside the bonds of trust that have traditionally connected the Canadian and American navies.

The Canadian navy began arranging to insert its ships into carrier battle groups in the late 1990s in an effort to improve interoperability with the U.S.

Navy (see figure 2). Initially, only West Coast ships, operating out of Canadian Forces Base Esquimalt, in British Columbia, were involved. The West Coast fleet

FIGURE 2

MARPAC Ships	
1995, HMCS *Calgary*	50 days as independent ship in MIF
1997, HMCS *Regina*	Surface action group
1998, HMCS *Ottawa*	*Abraham Lincoln* BG, fully integrated
1999, HMCS *Regina*	*Constellation* BG, replaced U.S. ship
2000, HMCS *Calgary*	Surface action group, PacMEF
2001, HMCS *Winnipeg*	*Constellation* BG, on-scene commander 17–24 July 02, TACON of all BG units
2001, HMCS *Vancouver*	*John C. Stennis* BG
MARLANT Ships	
2001, HMCS *Charlottetown*	LANTMEF, joined *Harry S. Truman* BG in Med.

MIF Maritime Interdiction Force
BG battle group
PacMEF Pacific Marine Expeditionary Force
TACON tactical control
LANTMEF Atlantic Marine Expeditionary Force

had fewer recurring operational commitments (such as the NATO Standing Naval Force Atlantic) than the East Coast command in Halifax, Nova Scotia. Further, the West Coast fleet had a long tradition of operating with the U.S. Navy and were therefore more doctrinally compatible with it than the Halifax squadrons, which had been primarily influenced by their long history of NATO operations.

Since their introduction, the integration of Canadian ships into CVBGs has been an evolutionary process. Canadian ships began as members of the Maritime Interdiction Force in the Persian Gulf, later gradually moving into actual battle groups as mutual familiarity improved. What started first as an operational initiative eventually gained an explicit strategic stature (in the Canadian context), when it became Department of National Defence policy to improve interoperability with its allies, particularly the United States. The department now seeks to develop and maintain "tactically self-sufficient units," capable of substantial military contributions while asserting their Canadian identity. (A ground-forces equivalent would be the role Canadian Coyote LAV IIIs, armored reconnaissance vehicles, played in Bosnia, Kosovo, and now Afghanistan.) Commodore Dan McNeil, Director for Force Planning and Programme Co-ordination, has recently remarked, "We will never be able to field strategic level forces. . . . We're not ever going to be in that game. We're going to be fielding tactical units. [However,] if you properly use tactical units, you can achieve strategic effect. That is what we are trying to do."[53]

A revolutionary aspect of these carrier battlegroup operations has been the fact that individual Canadian ships have often replaced American ones. This

arrangement has been of mutual benefit; the United States has been able to address its shortages of frigates and destroyers, and Canada has been afforded professional opportunities that it could not hope to obtain on its own. These opportunities include not only extended operations in groups larger than those the Canadian navy typically sends to sea but also exposure to assets not in the Canadian order of battle—carriers, cruisers, and nuclear submarines.

Canada has thus become a member of a select club, enjoying special access to the command and control concepts developed by the U.S. Navy as it travels down the road of network-centric warfare, as well as to military support not normally offered to allies. Finally, CVBG operations enable the Canadian navy to develop professional skills in the areas of littoral and interdiction operations, for which there is no opportunity in North American waters.

At the same time, such deployments stress the mutual dependencies and vulnerabilities that are central to every good coalition operation. For the Canadian navy, given the relative scarcity of Canadian ships (Canada has only twelve *Halifax*-class frigates), each unit deployed has value out of proportion to its ultimate contribution to a carrier battle group. Obviously, sending such ships into the Persian and Arabian Gulfs, as is typical, is far more dangerous than assigning them to the standard fisheries patrols in Canadian waters they would most likely be conducting otherwise. Similarly, by replacing an American ship with a Canadian one, rather than simply augmenting the group, the U.S. Navy is placing considerable trust in the professionalism and competence of Canadian crews; as one battle group commander has declared, "We need to be ready to go on game day—and when we play, every game is game day."[54] Accepting a Canadian ship into a battle group also constitutes a commitment to look after that ship.

To ensure that they are not liabilities for their new battle groups, Canadian ships participate in the same exercises and workups that all American ships do. Similarly, they carry the latest revisions of the Global Command and Control System–Maritime (GCCS-M) and conduct training to ensure that they can share and use the information and imagery distributed on that system. The Canadian navy has been increasingly challenged by such upgrades, however, due to the legacy systems on board its ships. The CCS330 system that controls the ship displays in the operations rooms of the *Halifax* frigates and *Iroquois*-class destroyers is a closed-architecture system based on a unique operating system and military-specific software and hardware. State of the art ten years ago, it is becoming increasingly a maintenance problem and, even more seriously, has a very limited capacity for integration with new systems. New capabilities, like GCCS-M, must be added to Canadian ships on a stand-alone basis. Canadian display terminals, as a result, cannot send or receive operational messages; tactical networking requires separate consoles; and the information provided by

systems like GCCS-M and the Canadian equivalent of the SIPRNET, known as MCOIN III, become effectively "stovepiped." The result is a cluttered operations room where decision makers must consult a number of systems in order to gather all the information necessary to perform their jobs—obviously not the most efficient arrangement in the heat of battle.[55]

Interestingly, the Canadian navy's effort to remain abreast of the fast-moving electronics revolution in command and control technologies is not being driven by American requirements. The United States is pleased that Canada strives to prevent gaps in capabilities. However, Canadian naval officers stress, it is the long history of naval cooperation and overall familiarity between the navies that has facilitated these exchanges, not the technical "kit" installed aboard Canadian ships.[56] The difficulties Canadian ships typically encounter in integrating themselves into American battle groups largely arise from the issue of accessibility.

"Not being interoperable means that you . . . are not in a position to derive power from the information age."

In battlegroup operations, as noted, the Coalition Wide Area Network is the principal means for coordinating action between Canadian and American ships; the U.S. Navy is gradually migrating its command, control, communications, planning, and execution functions to web and other digitally based delivery methods, notably the SIPRNET. However, CWAN and SIPRNET have mutual interface limitations. E-mail can pass between the two systems as long as the U.S. user has a CWAN account. Nevertheless, a security "firewall" strips off attachments before admitting messages into the CWAN. Thus a Canadian recipient may receive a commander's directive but not the supporting and amplifying information that originally accompanied it. Furthermore, messages from SIPRNET users without registered CWAN accounts will not reach Canadian ships, which may thereby miss important items.

The growing use of "chat" features to plan and coordinate has also been noted, and CWAN has such features. However, there is no interconnection between SIPRNET chat and CWAN chat. In order for a Canadian ship to participate in a session with American counterparts, a CWAN liaison officer must type into CWAN what was entered onto the SIPRNET system. Any attachment must be "air-gapped" onto CWAN, which can be quite a complicated procedure, involving multiple transfers between networks (SIPRNET to NATO Information Tactical Display System to MCOIN III).[57] As there is frequently only a single Canadian liaison officer on the carrier, accordingly, transfers between the two systems are likely to be delayed when that officer is not on watch.[58] Canada urges the U.S. flagships to man the CWAN terminal during these times, but it is likely

to be overlooked in periods of high operational tempo—just when the Canadian ships most need the information.

Finally, the web features of SIPRNET are limited on the CWAN side. CWAN supports web pages, but they contain only information placed there by coalition partners. In a U.S.-run operation, the majority of the information needed will be originating from the United States. There is no direct connection between SIPRNET web pages and CWAN web pages; web files must be "air-gapped." As a result, CWAN and MCOIN III are often out of date, sometimes by days. Furthermore, CWAN information is likely to be only a "snapshot" of that available to SIPRNET, without the functional links that it has on the U.S. side, limiting the ability of coalition officers to "surf" for more information. Finally, the carrier is usually the only U.S. ship in a battle group with a CWAN terminal, in which case it is the sole unit capable of posting information there—making it all the more possible that important information will not be posted at all.

TRUST AND UNILATERALISM

There may be nothing available but inefficient, work-around solutions to these problems. The real difficulty is not so much technical as policy oriented. The natural desire to protect sensitive information is at the root of all these issues, and it is not unique to the United States—MCOIN III is a Canada-only system, just as SIPRNET is U.S.-only. We should not expect this sensitivity to disappear any time soon; in fact, 11 September 2001 doubtless heightened it. Releasability software helps to move information onto coalition networks in a timely fashion, but they are not gateways to the information that American officers use on a day-to-day basis. This results in two quandaries for Canadian ships. First, they often operate without even basic operational-procedure manuals; some publications have not been classified as releasable to Canada or to the Coalition Wide Area Network. Without such formal guidance, U.S. officers are generally reluctant to release even what is seemingly innocuous data for fear of making mistakes that could have repercussions for their careers.[59] Second, since the makeup of a carrier battle group is not permanent, information-sharing protocols must be rebrokered for each deployment. Sometimes gaining access is a question of proving one's bona fides to the battle group; sometimes the battlegroup staff is simply unaware what information has been passed, or is otherwise available, to the Canadian ship. Often such problems are resolved when the battlegroup commander becomes aware of them, but the necessity to approach "the flag" for such matters highlights the impediments to network operations in a coalition environment.

The Canadian experience with U.S. carrier battle groups is instructive in both positive and negative senses for the overall question of network-centric

operations in a coalition environment. It is positive in demonstrating that despite technical limitations and differences between two navies, effective cooperation can be achieved in the modern naval environment. Once willingness to cooperate and a basis of trust between two forces has been established, technology is not an impassable barrier. Canada's close experience with the United States may be helpful to other navies. In its vision document *Leadmark,* the Canadian navy has proposed to develop a "Gateway C4ISR"* function that would allow less capable navies to integrate themselves into network-centric operations.[60] The Canadian navy has performed such a function in the past. During the Gulf War, among the deciding factors in the selection of Canada to lead the Combat Logistics Force were its excellent interoperability with the United States (a proposed French ship, *Doudart de Lagrée,* "lacked good communications interoperability"), its multinational crews, and its remaining legacy communications systems (with which Canadian ships could talk with more or less all warships present).[61] At present, Canadian ships play an important intermediary role in passing on information to other coalition partners in the Arabian Gulf.

However, there is a very large caveat—the relationship between the Canadian navy and the U.S. Navy took decades to evolve, and even so significant impediments remain to the seamless integration of forces that network-centric warfare demands. Further, while CVBGs must be prepared for all warfare eventualities, Canadian ships have participated predominantly in maritime interdiction. One wonders how welcome even Canadian ships might be in an operation dominated by strike warfare, against an asymmetric surface threat, in the littoral. Finally, the security demands of U.S. military networks are likely to be troublesome indeed for navies without the privileged access afforded to Canadian ships and crews on the basis of long-shared operational experience and a wealth of trust. Indeed, if the Canadian experience indicates that coalition network-centric operations are possible, it also indicates that the price of admission will remain very high. In a dynamic coalition environment, professional trust will be critical, and the height of the bar will be set by both technology and policy. Because of the crippling effect of slower networks or nonnetworked ships in such a setting, information releasability issues may be a stimulus to American unilateralism.

* C4ISR: command, control, communications, computers, intelligence, surveillance, and reconnaissance.

NOTES

1. David C. Gompert, Richard L. Kugler, and Martin C. Libicki, *Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs* (Washington, D.C.: National Defense Univ. Press, 1999).
2. S. C. Spring, Dennis M. Gormley, K. Scott McMahon, Kenneth Smith, and Daniel Hobbs, "Information Sharing for Dynamic Coalitions," VPSR Report 2836 (Arlington, Va.: Pacific Sierra Research, December 2000), pp. 5–6.
3. Robert Chekan [Col., CF], "The Future of Warfare: Clueless Coalitions?" unpublished paper (Toronto: Canadian Forces College, October 2001).
4. Spring et al., p. 6.
5. Thomas B. Barnett, "The Seven Deadly Sins of Network Centric Warfare," U.S. Naval Institute *Proceedings* (January 1999), p. 37.
6. James Tritten, "Revolutions in Military Affairs: Paradigm Shifts and Doctrine," *A Doctrine Reader,* Newport Paper 9 (Newport, R.I.: Naval War College Press, 1995).
7. Originally named the Tactical International Data Exchange (or TIDE, "good for cleaning up messy tactical pictures"), it later became known as Link 2 (given as "II" in roman numerals) in the Royal Navy, which was already using forms of data-sharing technology to distribute tactical information among its ships. As other NATO links became established, Link II became known as "Link 11" (i.e., eleven). Norman Friedman, *World Naval Weapons Systems 1997–1998* (Annapolis, Md.: Naval Institute Press, 1997), p. 28.
8. Norman Friedman, "CEC and Fleet Defence," *RUSI Journal* (October 2000).
9. Edward Smith, "Network-centric Warfare: What's the Point?" *Naval War College Review* 54, no. 1 (Winter 2001), p. 61.
10. *The Canadian Navy's Command and Control Blueprint to 2010* (Ottawa: National Defence Headquarters, June 2001), p. 12.
11. Elias Oxendine IV, "Managing Knowledge in the Battle Group Theatre Transition Process," (thesis, U.S. Naval Postgraduate School, Monterey, California, September 2000), p. 18.
12. *The Canadian Navy's Command and Control Blueprint to 2010*, pp. 11–12.
13. Oxendine, p. 18.
14. Richard Scott, "Survival of the Fittest," *Jane's Defence Weekly,* 23 January 2002.
15. William R. Pope [LTC, USA], "U.S. and Coalition Command and Control Interoperability for the Future" (thesis, U.S. Army War College, Carlisle, Penna., April 2001), p. 10.
16. *Observations on Network Centric Warfare,* pp. 5–6, www.dtic.mil/jcs/j6/education/warfare.html [29 January 2002].
17. "CEC Passes through Successful OpEval, Navy says," *Defense Daily,* 25 September 2001, p. 1.
18. Daniel Busch and Conrad J. Grant, "Changing the Face of War: The Co-operative Engagement Capability," *Sea Power* (March 2000), pp. 37–39.
19. Robert Kerno, "Co-operative Engagement Capability and the Interoperability Challenge," *Sea Power* (March 1999), pp. 45–47.
20. Pope, pp. 9–10.
21. Robert M. Stuart [Capt., USN], "Network Centric Warfare in Operation Allied Force: Future Promise or Future Peril?" (course paper, Department of Joint Military Operations, Naval War College, Newport, R.I., 16 May 2000), p. 8.
22. "Center Outlives Network Centric Warfare Concept's Challenges," *Defense Daily*, 23 March 2001.
23. Stuart, p. 7.
24. "Defense Watch," *Defense Daily,* 18 October 1999.
25. *The Canadian Navy's Command and Control Blueprint to 2010*, pp. 20–21.
26. Michael L. Morua [Lt. Cdr., USN], "The Carrier Battle Group Force: An Operator's Perspective," paper delivered at Engineering the Total Ship (ETS) 2000 Symposium, 21–23 March 2000, Gaithersburg, Md.; Gordon I. Peterson, "Ready to Go on Game Day: At Sea with the USS *Theodore Roosevelt* Battle Group," *Sea Power* (September 2001), p. 5, www.navyleague.org/seapower_mag/sept2001/ready_gameday.htm [12 February 2002].

27. Bryan Bender, Kim Berger, Andrew Koch, "Afghanistan's First Lessons," *Jane's Defence Weekly*, 19 December 2001.
28. Peter Howard, "The USN's Designer of Concepts," *Jane's Defence Weekly*, 3 October 2001.
29. Pope, p. 10.
30. Eric Francis Germain, "The Coming Revolution in NATO Maritime Command and Control," *MITRE Technical Papers* (Arlington, Va.: MITRE Corporation, 24 October 1997), pp. 3–4, www.mitre.org/support/papers/technet97/index.html [5 February 2002].
31. Joseph M. Ladymon, "Network Centric Warfare and Its Function in the Realm of Interoperability," *Acquisition Review Quarterly* (Summer 2001), p. 115.
32. "General Warns over Digitisation Split," *International Defence Review*, 1 January 2002; John Kiszely, "Achieving High Tempo: New Challenges," *RUSI Journal* (December 1999).
33. Smith, p. 3; Oxendine, p. 19.
34. R. H. Scales [Maj. Gen., USA], "Trust, Not Technology Sustains Coalitions," in Robert H. Scales, Williamson Murray, Paul K. Van Riper, and John A. Parmentola, *Future Warfare* (Carlisle, Penna.: U.S. Army War College, 1999).
35. Gary Wheatley [Rear Adm., USN (Ret.)], Diana Buck, "Multinational Command and Control: Beyond NATO," paper presented to 1999 Command and Control Research and Technology Symposium, Naval War College, Newport, R.I., p. 6.
36. Pope, p. 12.
37. Stuart, p. 7.
38. "General Warns over Digitisation Split."
39. Spring et al., p. 7.
40. See Gary McKerow, "Multilevel Security Networks: An Explanation of the Problem," *SANS Information Security Reading Room*, rr.sans.org/standards/multilevel.php, 5 February 2001, p. 2; Spring et al., pp. 29–34; Chekan, pp. 9–23.
41. Chekan, p. 11.
42. Henry S. Kenyon, "Alliance Forces Move toward Unified Data Infrastructure," *Signal* (September 2001).
43. Michael B. Black [Maj., USA], "Coalition Command, Control, Communications, Computer and Intelligence Systems Interoperability: A Necessity or Wishful Thinking?" (thesis, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas, 2 June 2000), pp. 5–6.
44. "Radiant Mercury," p. 1, www.fas.org/irp/program/disseminate/radiant_mercury.htm [5 February 2002]. For Siren, Bryan Bender, "JWID Puts Information Sharing System to the Test," *Jane's Defence Weekly*, 16 August 2001.
45. Spring et al., p. 17; Pope, p. 11; Nancy Hesson [Lt. (j.g.), USN], "Coalition Wide Area Network Allows Rapid Communications to RIMPAC's Multinational Force," *RIMPAC 2000*, RIMPAC Combined Information Bureau, www.cpf.navy.mil/rimpac2000/news/rimpac028.html [5 February 2002].
46. Wheatley and Buck, p. 9.
47. Quoted in Thomas Spierto [Lt. Cdr., USN], "Compromising the Principles of War: Technological Advancements Impact Multinational Military Operations" (course paper, Naval War College, Newport, R.I., 5 February 1999), p. 3.
48. See, for example, Robert W. Riscassi, "Principles for Coalition Warfare," *Joint Forces Quarterly* (Summer 1993).
49. Chekan, p. 4.
50. Pope, p. 6.
51. "General Warns over Digitization Split."
52. James Carr [Cdr., USN], "Network Centric Coalitions: Pull, Pass, or Plug-in?" (course paper, Naval War College, Newport, R.I., 15 May 1999), pp. 15–16.
53. Sharon Hobson, "Canada Aims for Defence Interoperability with the U.S.," *International Defence Review*, 1 January 2001.
54. Peterson, p. 7.
55. *The Canadian Navy's Command and Control Blueprint to 2010*, p. 17.
56. Reportedly, the U.S. Navy would like to extend the same level of cooperation to the Royal Australian Navy; however, the RAN faces considerably more difficulty in freeing up a ship for six-month workups with CVBG,

given the distances involved. For Canada the matter is simpler, given the proximity of Halifax and Esquimalt to American naval bases.

57. The process can become complicated, depending on the nationality and access of the liaison officer. Canadian officers would have access to the Combat Information Center and, though without access to SIPRNET, could at least retype into CWAN simultaneously, as liaison officers without access to CIC could not. However, American officers, who would have SIPRNET access, can man the CWAN station. "Air-gapping"—downloading data to a floppy disk for reentry into the other network.

58. In the present operations in the Arabian Gulf, there are frequently more Canadian officers aboard the U.S. carrier. This is because of the presence of a Canadian task group engaged in maritime interdiction and littoral interdiction operations. Similarly, given the coalition nature of the operations in South Asia, more liaison officers from other navies would be present to man the CWAN terminals. However, for a typical Canada/U.S. CVBG deployment, only a single officer would be present aboard the carrier.

59. Kevin O'Brien, "Europe Weighs Up Intelligence Options," *Jane's Intelligence Review*, 1 March 2001, p. 6.

60. *Leadmark: The Navy's Strategy for 2020* (Ottawa: Department of National Defence, 2001), p. 107.

61. Jean Morin [Maj.], Richard Gimblett [Lt. Cdr.], *Operation Friction* (Toronto: Dundurn Press, 1997), pp. 181–82; D. Miller [Commodore] and Sharon Hobson, *The Persian Excursion: The Canadian Navy in the Gulf War* (Clementsport, N.S.: Canadian Peacekeeping Press, 1995), p. 156.